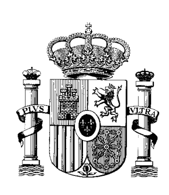


MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN



REF:	2009-17-INF-472 v1	Creado:	CERT8
Difusión:	Público	Revisado:	TECNICO
Fecha:	26.03.2010	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente:	2009-17 Borrado Seguro Anova
Datos del solicitante:	B83844373 Anova IT Consulting, S.L.

Referencias:	EXT-807	Solicitud de Certificación de Borrado Seguro Anova
	EXT-885	ETR de Borrado Seguro Anova v2.0.
	CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del producto Borrado Seguro Anova, versión 1.2.0, según la solicitud de referencia [EXT-807], de fecha 03/08/2009, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-885] de acuerdo a [CCRA], recibido el pasado18/12/2009.



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

INDICE



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto Borrado Seguro Anova, versión 1.2.0.

BSA realiza el borrado seguro de datos por método de sobreescritura sobre los dispositivos de almacenamiento seleccionados.

La aplicación genera, al final del proceso, un informe en el que se detallan las operaciones realizadas. Una vez finalizado el proceso de borrado seguro sobre un dispositivo de almacenamiento, los datos que éste contuviera no podrán ser recuperados con ningún método conocido.

Fabricante: Anova IT Consulting, S.L.

Patrocinador: Anova IT Consulting, S.L.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)

Laboratorio de Evaluación: Epoche & Espri

Perfil de Protección: Ninguno

Nivel de Evaluación: EAL1+ (ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, ALC_FLR.1)

Fortaleza de las Funciones: no aplica en CC v3.1

Fecha de término de la evaluación: 18/12/2009

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1+ (aumentado con ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, ALC_FLR.1) presentan el veredicto de "PASA". Por consiguiente, el laboratorio Epoche & Espri asigna el VEREDICTO de "PASA" a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1+, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Borrado Seguro Anova v1.2.0, se propone la resolución estimatoria de la misma.



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen del TOE

El producto Borrado Seguro Anova (**BSA**) es un sistema que permite realizar el borrado seguro de los datos contenidos en los dispositivos de almacenamiento conectado a un equipo.

BSA se presenta como un CD autoarrancable acompañado de una memoria extraíble USB donde está almacenado el paquete de licencias necesario para el funcionamiento de la aplicación.

BSA permite elegir de entre una serie de métodos predefinidos y métodos definidos por el usuario. Se puede seleccionar un método predefinido de entre los métodos más utilizados en cuanto a número de pasadas y caracteres empleados. Si se elige el método personalizado, el usuario puede definir tantas pasadas de borrado como precise. En cada una de las pasadas se definirá: el carácter empleado (fijo o aleatorio) y si se realiza la verificación tras el borrado. Siguiendo unas sencillas indicaciones permite iniciar el proceso de borrado de los dispositivos. Después del proceso de borrado y verificación (si existe) se generará auditoria referente al resultado del proceso de borrado.

Finalizado el proceso se presenta en pantalla el resultado del mismo y almacena dicho resultado en un archivo de texto para su comprobación posterior.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, más las requeridas para el componente adicional, ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, ALC_FLR.1, según la parte 3 de CC v3.1 r3.

ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance claims
ASE_OBJ.1	Security objectives for the operational environment
ASE_ECD.1	Extended components definition
ASE_REQ.1	Stated security requirements
ASE_TSS.1	TOE summary specification
ASE_SPD.1	Security Problem Definition
ASE_OBJ.2	Security Objetives
ASE_REQ.2	Derived Security Requirements
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labelling of the TOE
ALC_CMS.1	Parts of the TOE CM coverage
ALC_FLR.1	Basic Flaw Remediation



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ADV_FSP.1	Basic functional specification
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

FDP_RIP	Residual Information Protection
FMT_SMF	Specification of Management Functions
FAU_GEN	Security Audit Data Generation

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Identificación

Producto: Borrado Seguro Anova v1.2.0.

Declaración de Seguridad: Declaración de seguridad, Borrado Seguro Anova, v0.8

Perfil de Protección: Ninguno

Nivel de Evaluación: CC v3.1 r3 EA1+ (ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, ALC_FLR.1).

Fortaleza de las Funciones: no aplica en CC v3.1.

Política de seguridad

El uso del producto Borrado Seguro Anova, v1.2.0, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de las políticas como dispositivo de firma se encuentra en la declaración de seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Política 01: OSP1

Al finalizar el proceso de borrado se genera un informe en el que se recoge el log de actividades realizadas. Este informe se almacena en el primer sector del dispositivo borrado y puede salvarse en un dispositivo externo. Para su visualización en un equipo externo al sistema.

Hipótesis y entorno de uso

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

Para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Hipótesis 01: HIP1

La hora que utiliza el TOE para indicar el momento en el que se ha realizado cada actividad es aportada por el entorno con suficiente fiabilidad.

Hipótesis 02: HIP2

No se permite tomar el control del equipo con anterioridad a la ejecución del TOE, impidiendo así la posibilidad de ejecutar código malicioso que interfiera en la ejecución satisfactoria del TOE.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto Borrado Seguro Anova,v1.2.0, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a "Basic" de EAL1, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Amenazas cubiertas:

Amenaza 01: AM1

Después de ejecutar el proceso de borrado satisfactoriamente, cualquier atacante consigue comprometer la confidencialidad de los datos de usuario, accediendo a los datos almacenados previamente en los dispositivos borrados.

Funcionalidad del entorno.

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

Objetivo entorno 01: OE1

El entorno facilitará una fuente de tiempo suficientemente fiable en sus dos modos de obtención:

- Hora aportada por la BIOS del sistema

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Hora de un servidor externo de hora NTP

En el caso que la conexión a Internet no se encuentre habilitada en el informe se indicará como “No Disponible” en el apartado de Hora de Internet.

El objetivo de entorno 1 (OE1) cumple la hipótesis 1(HIP1)

Objetivo entorno 02: OE2

El entorno debe garantizar que no se ejecuta código malicioso que interfiera en la práctica satisfactoria del TOE.

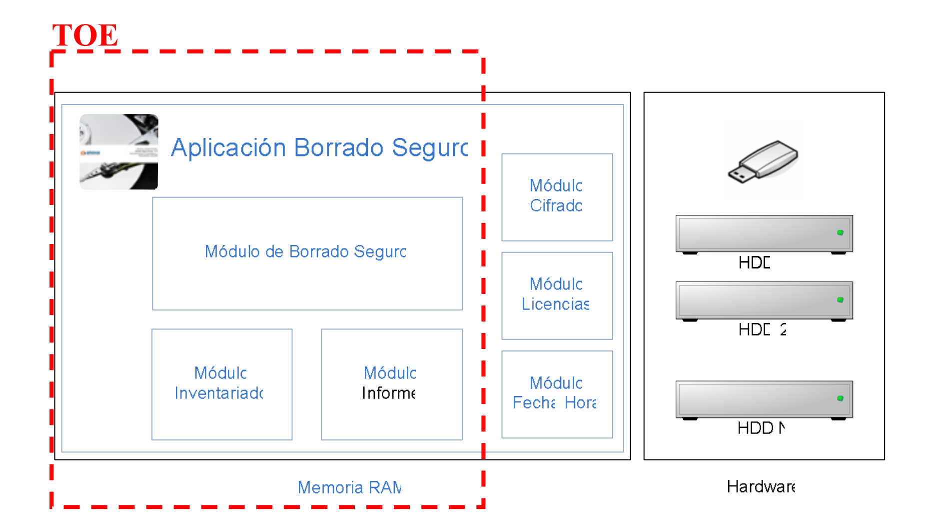
El objetivo de entorno 2 (OE2) cumple la hipótesis 1(HIP2).

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del OE se encuentran en la correspondiente Declaración de Seguridad.

Arquitectura

Arquitectura:

El TOE es una aplicación SW, por lo que todo el Hardware y Firmware queda excluido del mismo formando parte del entorno. Al ser una aplicación autoejecutable que se carga durante el arranque del sistema desde CD, no existe ningún SW externo con el que interactúe.



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Documentos

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Manual de usuario v0.7, diciembre 2009

Pruebas del producto

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todos las pruebas ha sido realizados por el fabricante en sus instalaciones con resultado satisfactorio.

El proceso ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la declaración de seguridad.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido entorno a un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

Configuración evaluada

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto Borrado Seguro Anova, v1.2.0 es necesario disponer de los siguientes componentes:

- Máquina X86 con lector de dispositivo óptico disponible
- RAM minima: 128 Mb
- Discos Duros tipo IDE y SATA.

Dentro de todas las posibilidades que ofrecen estos requisitos, las configuraciones que se han elegido para su evaluación son las siguientes:

TIPO	FABRICANTE	MODELO	INTERFACE	CAPACIDAD
Disco Duro	WESTERN DIGITAL	WD400BB	IDE	40 GB
Disco Duro	WESTERN DIGITAL	WD400BD	SATA	40 GB
Disco Duro	MAXTOR	31024H1	IDE	10 GB
Disco Duro	SEAGATE	ST3802110A	IDE	80 GB
Disco Duro	SEAGATE	ST380013AS	SATA	80 GB
Controladora	Intel® 82801E	Communications I/O	SATA/IDE	

Resultados de la Evaluación

El producto Borrado Seguro Anova, v1.2.0 ha sido evaluado frente a la declaración de seguridad “Declaración de Seguridad Borrado Seguro Anova”, v0.8 de diciembre de 2009.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL1+** (aumentado con ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, ALC_FLR.1) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1+, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r3.

Recomendaciones y comentarios de los evaluadores

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- La marca de borrado de los dispositivos podría llegarse a falsear, y por lo tanto no existiría plena certeza de si un producto ya ha sido borrado con anterioridad, hecho que se avisa en los manuales del producto. Por lo tanto, se recomienda utilizar otras medidas para saber si ya se ha borrado un dispositivo. Esta situación se acentúa por la facilidad para encontrar la clave de cifrado de los informes.

- A pesar de que el TOE arranca desde CD, sigue sin existir una cadena de confianza que permita un arranque seguro, por lo tanto, el TOE no debe ser usado en un PC que haya sido comprometido con anterioridad. Esta vulnerabilidad se ha mitigado mediante una suposición del entorno.

- Existen ciertas memorias USB con un hardware especial que simula una unidad de CD (dispositivos U3). En el caso de utilizar el TOE para borrar uno de estos dispositivos, será imposible borrar correctamente la parte marcada como correspondiente al CD simulado.

- El TOE no borra dispositivos SCSI.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Borrado Seguro Anova, v1.2.0, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ETR	Evaluation Technical Report
OC	Organismo de Certificación
CD	Compact Disk
USB	Universal Serial Bus
IDE	Integrated Drive Electronics
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Bibliografía

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Evaluation methodology, Version 3.1, r3, July 2009.

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: **Declaración de Seguridad Borrado Seguro Anova v1.2.0, v0.8 diciembre 2009**.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es